**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

Claims 1-19. (canceled).

20. (currently amended) A method for protecting the processing of sensitive information in a security module having a monolithic structure comprising at least an information processing device, a storage device for storing information capable of being processed by said processing device and at least a data bus, the security module further comprising means for checking the integrity of information, said means for checking the integrity being either a table contained in the processing device or a plurality of software program instructions of the storage device or a specific hardware circuit, the method comprising at least the following steps:

selecting a piece of sensitive information stored in the storage device addressed by the processing means;

determining, by the means for checking the integrity, a specific condition for establishing the integrity of said sensitive information to be transmitted on said data bus;

transferring a datum of said sensitive information from the storage device to the processing device, on said data bus;

verifying said datum transferred on said data bus, by said means for checking the integrity for verifying that said specific condition is satisfied; and

disabling the processing of said sensitive information by the processing device if the specific condition is not satisfied.

wherein said datum of said sensitive information is an operation code datum read in the storage device, said operation code datum being recognized in said table contained in the processing device, said specific condition being satisfied if said operation code datum is equal to a valid operation code datum of the table and said specific condition is not satisfied at least if bits of the operation code datum are all equal to a same binary value.

Claims 21–25. (canceled)

26. (previously presented) The method according to claim 20, wherein the disabling of the processing of said sensitive information comprises the disabling of the processing device performed by executing a microprogrammed instruction.

27. (previously presented) The method according to claim 26, wherein said microprogrammed instruction induces the following steps:

- writing a piece of disable data into a non volatile location of the storage device; and

- disabling the processing device.

28. (previously presented) The method according to claim 27, wherein said microprogrammed instruction further comprises the reading by the processing device at said non volatile location of the storage device upon power up of said module, before disabling the processing device if a value read at this location does not match.

29. (currently amended) A security module comprising an electronic circuit having a monolithic structure and comprising an information processing device, an information storage device communicating with said processing device via a data bus, the processing device selecting sensitive information data extracted from the storage

device in order to process them, the security module further comprising means for checking the integrity of information being either a table contained in the processing device or a plurality of software program instructions of the storage device or a specific hardware circuit, wherein said means for checking the integrity verifies a specific condition for integrity by verifying a datum of said sensitive information, transferred on the data bus, the security module further comprising means for disabling the processing of said sensitive information by the processing device when said specific condition for integrity is not satisfied,

wherein the datum transferred on the data bus is an operation code datum executed by the processing device corresponding to an instruction extracted from said table, the table comprising at least a forbidden instruction, and

wherein said specific condition for integrity is not satisfied when said processing device processes said forbidden instruction.

30. (canceled)

31. (currently amended) The security module according to claim ~~30~~ 29, wherein at least instructions of said table corresponding to operation code datum constituted by bits all equal to a same binary value are forbidden instructions of said table.

32. (canceled)

33. (previously presented) The security module according to claim 29, wherein said means for disabling the processing of said sensitive information comprises means for irreversibly writing at least one indicator with an initial valid state in a non reversible modified invalid state, and means for reading said indicator

during the next power-up of the module and disabling the processing device if an invalid state of said indicator is read.

Claims 34-36. (canceled)

37. (previously presented) The security module according to claim 33, wherein said irreversibly writing of said indicator is performed by executing a microprogrammed instruction.

38. (previously presented) The security module according to claim 29, wherein said security module is a microcircuit card.

Claims 39-41. (canceled)

42. (previously presented) The method according to claim 20, wherein when determining of a specific condition for the integrity of said information, at least two software instructions of the storage means are executed by processing means for determining said specific condition.

43. (previously presented) The method according to claim 20, wherein when determining of a specific condition for the integrity of said information, the means for checking integrity of information comprises a specific hardware circuit for checking integrity of information in entry of the data bus and at output of the data bus.

44. (previously presented) The security module according to claim 29, wherein the means for checking the integrity comprises at least two software instructions executed by the processing means for verifying said specific condition for integrity.

45. (previously presented) The security module according to claim 29, wherein the means for checking the integrity comprise a specific hardware circuit for checking integrity of information in entry of the data bus and at output of the data bus for verifying said specific condition for integrity.

46. (new) A method for protecting the processing of sensitive information in a security module having a monolithic structure comprising at least an information processing device a storage device for storing information capable of being processed by said processing device and at least a data bus, the security module further comprising means for checking the integrity of information, said means for checking the integrity being either a table contained in the processing device or a plurality of software program instructions of the storage device or a specific hardware circuit, the method comprising at least the following steps:

selecting a piece of sensitive information stored in the storage device addressed by the processing means;

determining, by the means for checking the integrity, a specific condition for establishing the integrity of said sensitive information to be transmitted on said data bus;

transferring a datum of said sensitive information from the storage device to the processing device, on said data bus;

verifying said datum transferred on said data bus, by said means for checking the integrity for verifying that said specific condition is satisfied; and

disabling the processing of said sensitive information by the processing device if the specific condition is not satisfied,

wherein said means for checking the integrity comprises a first and a second logic operator disposed in an entry and an output of the data bus, respectively, and producing a first and a second result, respectively, the means for checking the integrity further comprising a logic comparator for comparing said first and second result, and for verifying said specific condition for the integrity by checking an equality between said first and second results.

47. (new) The method according to claim 46, wherein said first and second logic operators are parity generators each having two logic opposite outputs and one logic selection input that determines which of said two logic opposite outputs is input in the comparator.

48. (new) The method according to claim 47, wherein said logic selection input of the comparators is set to a calculation data whose value varies as a function of time.

49. (new) The method according to claim 47, wherein said logic selection input of both comparators is set to a calculation data whose value varies randomly.

50. (new) A security module comprising an electronic circuit having a monolithic structure and comprising an information processing device, an information storage device communicating with said processing device via a data bus, the processing device selecting sensitive information data extracted from the storage device in order to process them, the security module further comprising means for checking the integrity of information being either a table contained in the processing device or a plurality of software program instructions of the storage device or a specific hardware circuit, wherein said means for checking the integrity verifies a

specific condition for integrity by verifying a datum of said sensitive information, transferred on the data bus, the security module further comprising means for disabling the processing of said sensitive information by the processing device when said specific condition for integrity is not satisfied,

wherein said means for checking the integrity of information comprises a first and a second parity generator respectively disposed in an entry and an output of the data bus, and a comparator whose inputs are connected to outputs of said first and second parity generators to verify said specific condition for integrity when said first and second parity generators produce identical outputs, and to set an output of said comparator linked to an interrupt input of the processing device.

51. (new) The security module according to claim 50, wherein said outputs of said first and second parity generators are set opposite according to a function of time.

52. (new) The security module according to claim 50, wherein said outputs of said first and second parity generators are set opposite randomly.